Terror Preparedness Action Plan
(for Company Management and Business Owners)

As company management and business owners, you play a crucial role in encouraging preparedness initiatives during peacetime. You have the capability to create a security-focused workplace culture, and implement business continuity plans.

PREVENTION

Prepare Your Workforce

☐ *Improve Emergency Preparedness Skills and Knowledge*
- ○ Download the SGSecure mobile app
- ○ Utilise resources on the SGSecure@Workplaces website
- ○ Put up "Run-Hide-Tell" and "Press-Tie-Tell" posters
- ○ Send frontline employees for emergency skills training
- ○ Incentivise employees who participate in drills and exercises
- ○ Frequently test and remind employees about emergency and safety procedures

☐ *Empower People to Address Threats of Terrorism*
- ○ Appoint and register an SGSecure Rep

Protect Your Workplace

☐ *Physical Measures*
- ○ Install functioning CCTVs in shops

☐ *Operational Measures*
- ○ Create a risk management plan
- ○ Regularly review security policies
- ○ Hire third-party auditors to conduct cross checks
- ○ Hold post-audit meetings with stakeholders
- ○ Get bizSAFE recognition
- ○ Establish HR guidelines to support employees after an attack

☐ *Cybersecurity Measures*
- ○ Use application control software
- ○ Check computers regularly and inspect emails
- ○ Record where sensitive data is stored
- ○ Back up data periodically

☐ *Business Continuity Management*
- ○ Create and review business continuity plans
- ○ Participate in the Corporate First Responder (CFR) Scheme
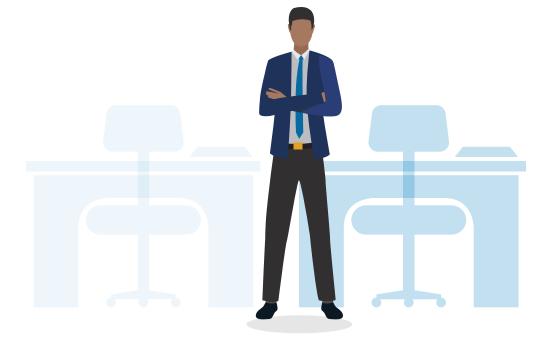
Partner Your Community

☐ *Employees Bonding and Cohesion*
- ○ Organise team-building activities for employees
- ○ Communicate regularly with frontline employees

☐ *External Networks and Stakeholders*
- ○ Prepare a list of business partners (including unions, where applicable) who can support business operations after an attack

☐ *Crisis Communication Plans*
- ○ Create and maintain an authoritative source of company information
- ○ Refer only to authoritative sources of information
- ○ Create and update employee and next-of-kin call directories
- ○ Create a list of individuals to contact during a crisis
- ○ Establish procedures to disseminate information to employees and colleagues
- ○ Organise a company crisis response team
- ○ Appoint a company spokesperson

RESPONSE

Terror Attacks

☐ *Activating Teams and Response Protocols*

○ Assemble your Crisis Response Team

○ Inform the police, employees, and neighbouring tenants of the attack

☐ *Inform Others of the Attack*

○ Call 999 or SMS 71999 to inform the police

○ Submit information through the SGSecure App

○ Alert other nearby outlets of the attack

○ Prepare a media release and factsheet

☐ *Evacuate the Premises*

○ Cooperate with CERT Team in evacuation procedures

☐ *Provide Information*

○ Coordinate communication between outlets and employees

☐ *Assist Others*

○ Use Press, Tie, Tell for improvised first aid

○ Assist the police with investigations

Cyber Attacks

☐ *Responding to Cyber Incidents*
A cyber incident is an event that indicates harm or the attempt to do harm to a company's system.

○ Execute roles and responsibilities spelt out in the company's Incident Response Plan, which may call for people to do the following:

○ Contain:
  - Keep track of the company's incident handling process (e.g. walk-through the pre-prepared Incident Response Plan to ensure that steps are executed, information is gathered, etc.)
  - Limit the impact of an incident by acting fast on the course of action (e.g. notifying the right personnel, isolating the infected or compromised system, etc.)
  - Report the incident to the relevant authorities or organisations (e.g. if monetary loss is involved, lodge a police report and alert the bank immediately)

○ Eradicate:
  - Resolve the issue (e.g. removing malware, patch machines with the same potential vulnerability, etc.)
  - Complete forensic analysis and keep logs

○ Recover:
  - Restore business functions (e.g. setting up a new system, restoring from clean backups)
  - Monitor the recovered system to be certain that incident has been fully resolved
  - Gather the lessons learnt and improve the company's Incident Response Plan

RECOVERY

Supporting Employees and Colleagues

○ Rally employees and colleagues together

○ Set up support groups for affected employees

○ Perform Psychological First Aid for traumatised employees

○ Provide access to professional support for employees who require it

○ Update employees on measures taken to safeguard their well-being

○ Execute pre-established HR guidelines to manage fallout

Discerning Between Information Sources

○ Activate pre-established crisis communication plans

○ Check and verify information about the attack from official sources before informing employees and concerned family members

○ Refrain from, and prohibit the sharing of videos or photos which may fuel rumours

○ Address potential cases of discrimination or shunning among employees

Pooling Resources Together

○ Activate business continuity plans

○ Contact contractors and suppliers to assist in business operations and recovery

○ Get in touch with key partners such as unions, where applicable

○ Work with the building manager to coordinate reopening of businesses

○ Discuss learning points from incidents with employees and colleagues